

Nilpotent linearized polynomials over finite fields and applications

Lucas Reis

Departamento de Matemática, Universidade Federal de Minas Gerais, UFMG, Belo Horizonte, MG, 30123-970, Brazil

Abstract

Let q be a prime power and \mathbb{F}_{q^n} be the finite field with q^n elements, where $n > 1$. We introduce the class of the linearized polynomials $L(x)$ over \mathbb{F}_{q^n} such that

$$L^{(t)}(x) := \underbrace{L(L(\cdots(x)\cdots))}_{t \text{ times}} \equiv 0 \pmod{x^{q^n} - x}$$

for some $t \geq 2$, called *nilpotent linearized polynomials* (NLP's). We discuss the existence and construction of NLP's and, as an application, we show how to construct permutations of \mathbb{F}_{q^n} from these polynomials. For some of those permutations, we can explicitly give the compositional inverse map and the cycle structure. This paper also contains a method for constructing involutions over binary fields with no fixed points, which are useful in block ciphers.

Keywords: Linearized polynomials, Permutation polynomials, Cycle structure, Involutions
 2010 MSC: 12E20, 11T06

1. Introduction

Let q be a prime power and \mathbb{F}_{q^n} be the finite field with q^n elements, where $n > 1$. Any map from \mathbb{F}_{q^n} to itself can be represented by a polynomial in $\mathbb{F}_{q^n}[x]$. Conversely, any polynomial in $\mathbb{F}_{q^n}[x]$ induces a map from \mathbb{F}_{q^n} to itself. In this context, the \mathbb{F}_q -linear maps of \mathbb{F}_{q^n} corresponds to the so called linearized polynomials $L(x) = \sum_{i=0}^k a_i x^{q^i}$, $a_i \in \mathbb{F}_{q^n}$. If a polynomial $f(x) \in \mathbb{F}_{q^n}[x]$ induces a permutation in \mathbb{F}_{q^n} we say that $f(x)$ is a permutation polynomial over \mathbb{F}_{q^n} . For many applications in coding theory [2] and cryptography [5], it is interesting to find new families of permutation polynomials over finite fields. For instance, in block ciphers, permutations of binary fields are used as S-boxes to build a confusion layer in the encryption process and the inverse of this permutation is used in the decryption process. In order to avoid some problems like limited memory, it is interesting to use involutions of binary fields, i.e., permutation polynomials $f(x) \in \mathbb{F}_{2^n}[x]$ such that $f^{-1}(x) = f(x)$ or, equivalently, $f(f(x)) = x$. However, a random permutation in \mathbb{F}_{2^n} has $O(1)$ fixed points, while a random involution has $2^{n/2} + O(1)$ fixed points. Therefore an involution with more than $O(1)$ fixed points can be distinguished from random permutations and so can be attacked. In fact, as it was suggested in

Email address: lucasreismat@gmail.com (Lucas Reis)

[1], the involutions should have no fixed points. For more information about construction and properties of permutation polynomials, see [4].

In this paper we introduce the class of the *nilpotent linearized polynomials* (NLP's), i.e., linearized polynomials $L(x) \in \mathbb{F}_{q^n}[x]$ such that

$$L^{(t)}(x) \equiv 0 \pmod{x^{q^n} - x}$$

for some $t \geq 2$, where $L^{(t)}(x)$ denotes the ordinary polynomial composition of $L(x)$ with itself t times.

We study the existence and construction of those polynomials, including explicit examples. We describe a method for constructing permutation and complete permutation polynomials from those nilpotent polynomials and, in some particular cases, we determine the compositional inverse map and describe the cycle structure. This paper also includes explicit examples of involutions over binary fields which have no fixed points.

2. Existence and properties of NLP's

Throughout this paper, \mathbb{F}_{q^n} denotes the finite field with q^n elements, where q is a prime power and $n > 1$. A polynomial $L(x) \in \mathbb{F}_{q^n}[x]$ is said to be *linearized* if $L(x) = \sum_{i=0}^k a_i x^{q^i}$. Notice that if $L(x)$ is linearized, then $L(z+y) = L(z) + L(y)$ and $L(az) = aL(z)$ for any $a \in \mathbb{F}_q$ and $y, z \in \mathbb{F}_{q^n}$, hence $L(x)$ induces an \mathbb{F}_q -linear map of \mathbb{F}_{q^n} . Conversely, if $\{\omega_1, \dots, \omega_n\}$ is any basis of \mathbb{F}_{q^n} over \mathbb{F}_q , then the matrix $D = (\omega_i^{q^{j-1}})_{ij}$ is invertible and then, for any \mathbb{F}_q -linear map M of \mathbb{F}_{q^n} we have that $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ is the linearized polynomial representation of M , where

$$(a_0, \dots, a_{n-1})^T = D^{-1}(b_1, \dots, b_n)^T,$$

$b_i = M(\omega_i)$ and T denotes the transpose. This is an one-to-one correspondence between the \mathbb{F}_q -linear maps of \mathbb{F}_{q^n} and the linearized polynomials $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_{q^n}[x]$.

Remark 1. If $L(x) = \sum_{i=0}^k a_i x^{q^i} \in \mathbb{F}_{q^n}[x]$ and $k > n-1$, then the \mathbb{F}_q -linear map of \mathbb{F}_{q^n} induced by $L(x)$ can be represented by another linearized polynomial of the form $L_0(x) = \sum_{i=0}^{n-1} b_i x^{q^i} \in \mathbb{F}_{q^n}[x]$. In fact, $L_0(x)$ is the reduction of $L(x)$ modulo $x^{q^n} - x$. For this reason we will be mostly interested in the linearized polynomials of the form $\sum_{i=0}^{n-1} a_i x^{q^i}$.

Definition 1. If $t \geq 2$ is an integer, we say that $L(x) \in \mathbb{F}_{q^n}[x]$ is a t -nilpotent linearized polynomial (t -NLP) over \mathbb{F}_{q^n} if $L(x)$ is a linearized polynomial such that $L(x) \not\equiv 0 \pmod{x^{q^n} - x}$ and

$$L^{(t)}(x) \equiv 0 \pmod{x^{q^n} - x}.$$

In other words, $L^{(t)}(x)$ is the zero function when restricted to \mathbb{F}_{q^n} and $L(a) \neq 0$ for some $a \in \mathbb{F}_{q^n}$.

It follows from definition that $L(x)$ is a t -NLP over \mathbb{F}_{q^n} if, and only if, its polynomial reduction modulo $x^{q^n} - x$ is a t -NLP over \mathbb{F}_{q^n} . Moreover, any t -NLP is also a d -NLP for every $d > t$.

If $f(x) \in \mathbb{F}_{q^n}[x]$, we denote $Z_f = \{z \in \mathbb{F}_{q^n} | f(z) = 0\}$ the set of the roots of $f(x)$ in \mathbb{F}_{q^n} and $V_f = \{f(z); z \in \mathbb{F}_{q^n}\}$ its value set over \mathbb{F}_{q^n} . If $L(x)$ is a linearized polynomial over \mathbb{F}_{q^n} , then V_L

and Z_L are \mathbb{F}_q -vector spaces. In fact V_L and Z_L are, respectively, the image and the kernel of the linear map of \mathbb{F}_{q^n} induced by L .

The following theorem gives a necessary and sufficient condition for the existence of t -NLP's over \mathbb{F}_{q^n} with prescribed value set V .

Theorem 1. *Let $V \subseteq \mathbb{F}_{q^n}$ be any \mathbb{F}_q -vector space. Then there exist an integer $t \geq 2$ and a t -NLP over \mathbb{F}_{q^n} such that $V = V_L$ if, and only if, $V \neq \{0\}, \mathbb{F}_{q^n}$.*

Proof. Suppose that $t \geq 2$ and $L(x)$ is a t -NLP over \mathbb{F}_{q^n} such that $V = V_L$. Notice that $L(a) \neq 0$ for some $a \in \mathbb{F}_{q^n}$, hence $V_L \neq \{0\}$. Since $L^{(t)}(z) = 0$ for any $z \in \mathbb{F}_{q^n}$, the \mathbb{F}_q -linear map of \mathbb{F}_{q^n} induced by $L(x)$ cannot be an isomorphism, hence $Z_L \neq \{0\}$ and then $V_L \neq \mathbb{F}_{q^n}$. Conversely, suppose that $V \neq \{0\}, \mathbb{F}_{q^n}$ and let $\{\omega_1, \dots, \omega_k\}$ be any basis of V over \mathbb{F}_q ; clearly $k \neq 0, n$. Let $\omega_{k+1}, \dots, \omega_n$ be elements of \mathbb{F}_{q^n} such that $\{\omega_1, \dots, \omega_n\}$ is a basis of \mathbb{F}_{q^n} over \mathbb{F}_q and M be the \mathbb{F}_q -linear map of \mathbb{F}_{q^n} defined as follows:

$$M(\omega_i) = \begin{cases} \omega_1 & \text{if } i = n \\ \omega_{i+1} & \text{if } 1 \leq i \leq k-1 \\ 0 & \text{if } k \leq i \leq n-1. \end{cases}$$

Since $0 < k < n$ and $n > 1$, M is well defined and a direct calculation shows that $V_M = V$ and $M^{(k+1)}(\omega_i) = 0$ for any $1 \leq i \leq n$. Hence $M^{(k+1)}(z) = 0$ for any $z \in \mathbb{F}_{q^n}$. Then $L(x) \in \mathbb{F}_{q^n}[x]$, the linearized polynomial representation of M , is a $(k+1)$ -NLP over \mathbb{F}_{q^n} and satisfies $V_L = V$. \square

As it was noticed at the beginning of this section, for a given basis of \mathbb{F}_{q^n} over \mathbb{F}_q , the construction of the linearized polynomial associated to a linear map requires only the calculation of the inverse of a matrix. In this context, the proof of Theorem 1 suggests a computational method for constructing t -NLP's with a given value set. However, we can find explicit examples of such polynomials:

Example 1. Let $\text{Tr}_{L/K}(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{q^{im}}$ be the trace of $L = \mathbb{F}_{q^n}$ over an subfield K of the form \mathbb{F}_{q^m} . If θ is an element of $\mathbb{F}_{q^n}^*$ such that $\text{Tr}_{L/K}(\theta) = 0$, then

$$L_\theta(x) = \theta \cdot \text{Tr}_{L/K}(x)$$

is a 2-NLP over \mathbb{F}_{q^n} and its value set over \mathbb{F}_{q^n} is given by $\theta \cdot \mathbb{F}_{q^m}$. In particular, if $\frac{n}{m}$ is divisible by $p = \text{char}(\mathbb{F}_q)$, then $L(x) = \text{Tr}_{L/K}(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{q^{im}}$ is a 2-NLP over \mathbb{F}_{q^n} .

Example 2. Let m be any positive integer and $n = 2m$. If α and β are two elements in $\mathbb{F}_{q^n}^*$ such that $\alpha^{q^m} + \alpha = 0$ and $\beta^{q^m+1} = 1$, a direct calculation shows that

$$L_{\alpha,\beta}(x) = \alpha\beta x^{q^m} + \alpha x$$

is a 2-NLP over \mathbb{F}_{q^n} . The equations $x^{q^m} + x = 0$ and $x^{q^m+1} = 1$ have, respectively, $q^m - 1$ and $q^m + 1$ solutions over $\mathbb{F}_{q^n}^*$. Hence there are $q^n - 1$ polynomials of the form $L_{\alpha,\beta}(x)$.

2.1. NLP's in $\mathbb{F}_q[x]$

Here we give a complete characterization of the t -NPL's over \mathbb{F}_{q^n} such that their coefficients lie on the base field, i.e, $L(x) \in \mathbb{F}_q[x]$. First we need to recall some concepts of the theory of linearized polynomials which can be found in [3], Section 3.4.

Definition 2. If $L_1(x), L_2(x) \in \mathbb{F}_{q^n}[x]$ are linearized polynomials we define their symbolic product by

$$L_1(x) \otimes L_2(x) = L_1(L_2(x)),$$

which also is a linearized polynomial.

A simple calculation shows that the symbolic product \otimes is associative, distributive with respect to the ordinary addition, but is not commutative. However, if $L_1(x), L_2(x) \in \mathbb{F}_q[x]$ it can be verified that $L_1(x) \otimes L_2(x) = L_2(x) \otimes L_1(x)$.

Definition 3. Let $L(x) = \sum_{i=0}^t a_i x^{q^i} \in \mathbb{F}_{q^n}[x]$ be a linearized polynomial and $l(x) = \sum_{i=0}^t a_i x^i$. The polynomials $l(x)$ and $L(x)$ are called q -associates of each other. More specifically, $l(x)$ is called the conventional q -associate of $L(x)$ and $L(x)$ is called the linearized q -associate of $l(x)$.

The following lemma shows an interesting property of the linearized polynomials $L(x) \in \mathbb{F}_q[x]$:

Lemma 1 ([3], Lemma 3.59). Let $L_1(x)$ and $L_2(x)$ be linearized polynomials with conventional q -associates $l_1(x)$ and $l_2(x)$, respectively. If the coefficients of L_1 and L_2 lie on the base field \mathbb{F}_q , then the polynomials $l(x) = l_1(x) \cdot l_2(x)$ and $L(x) = L_1(x) \otimes L_2(x)$ are q -associates.

Using Lemma 1 and the following proposition we will give necessary and sufficient conditions in order for $L(x)$ to be a t -NPL over \mathbb{F}_{q^n} in the case when $L(x) \in \mathbb{F}_q[x]$.

Proposition 1. Suppose that the polynomial $g(x) \in \mathbb{F}_q[x]$ satisfies $g(x+a) = g(x)$ for every $a \in \mathbb{F}_{q^n}$. Then there exists a polynomial $R(x) \in \mathbb{F}_q[x]$ such that $g(x) = R(x^{q^n} - x)$. In particular, if $g(x)$ is linearized, then so is $R(x)$.

Proof. For the first statement, we proceed by induction on $n = \deg g(x)$. If $g(x)$ is constant then there is nothing to prove. Suppose that the statement is true for all polynomials of degree at most k and let $g(x) \in \mathbb{F}_q[x]$ a polynomial of degree $k+1$ satisfying $g(x+a) = g(x)$ for every $a \in \mathbb{F}_{q^n}$. We have $g(0) = g(a)$ for all $a \in \mathbb{F}_{q^n}$ and so the polynomial $g(x) - g(0)$ has degree $k+1 > 0$ and vanishes at \mathbb{F}_{q^n} . In particular we have that

$$g(x) - g(0) = (x^{q^n} - x)G(x) \tag{1}$$

for some non-zero polynomial $G(x) \in \mathbb{F}_q[x]$. Since $g(x+a) - g(0) = g(x) - g(0)$ and $(x+a)^{q^n} - (x+a) = x^{q^n} - x$ for every $a \in \mathbb{F}_{q^n}$, it follows from (1) that $G(x) = G(x+a)$ for every $a \in \mathbb{F}_{q^n}$ and $\deg G(x) < \deg g(x)$. By the induction hypothesis we have that $G(x) = F(x^{q^n} - x)$ for some $F(x) \in \mathbb{F}_q[x]$. Therefore $g(x) = (x^{q^n} - x)F(x^{q^n} - x) + g(0)$ and so $g(x) = R(x^{q^n} - x)$, where $R(x) = xF(x) + g(0) \in \mathbb{F}_q[x]$.

For the second statement, notice that if $g(x)$ is linearized, then the equality $g(x) = R(x^{q^n} - x)$ yields:

$$bR(z^{q^n} - z) = bg(z) = g(bz) = R((bz)^{q^n} - bz) = R(b(z^{q^n} - z)) \quad (2)$$

$$R(z^{q^n} - z) + R(y^{q^n} - y) = g(z) + g(y) = g(z + y) = R(z^{q^n} - z + (y^{q^n} - y)) \quad (3)$$

for any $b \in \mathbb{F}_q$ and $y, z \in \overline{\mathbb{F}_{q^n}}$, where $\overline{\mathbb{F}_{q^n}}$ denotes the algebraic closure of \mathbb{F}_{q^n} . In particular, for any $A, B \in \overline{\mathbb{F}_{q^n}}$ there exist A_0 and B_0 in $\overline{\mathbb{F}_{q^n}}$ such that $A_0^{q^n} - A_0 = A$ and $B_0^{q^n} - B_0 = B$ and then, from the equalities (2) and (3), we conclude that

$$R(A + B) = R(A) + R(B) \quad \text{and} \quad R(bA) = bR(A)$$

for any $b \in \mathbb{F}_q$ and $A, B \in \overline{\mathbb{F}_{q^n}}$. Hence $R(x)$ induces an \mathbb{F}_q -linear map T from $\overline{\mathbb{F}_{q^n}}$ to itself. Let $r = \deg R(x)$ and s large enough such that $q^s > r$. If $S(x)$ is the linearized polynomial representation of T when restricted to \mathbb{F}_{q^s} , then $R(z) = S(z)$ for any $z \in \mathbb{F}_{q^s}$ and $\deg R, \deg S < q^s$. Therefore $R(x) = S(x)$ and thus $R(x)$ is linearized. \square

The main result of this section is the following:

Theorem 2. *Let $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_q[x]$ be a nonzero linearized polynomial and $l(x) = \sum_{i=0}^{n-1} a_i x^i$ its conventional q -associate. Then $L(x)$ is a t -NLP over \mathbb{F}_{q^n} if, and only if, $x^n - 1$ divides $l(x)^t$. In particular, if n is not divisible by p then for any $t \geq 2$, there are no t -NLP's over \mathbb{F}_{q^n} with coefficients in \mathbb{F}_q .*

Proof. Suppose that $l(x)^t = (x^n - 1) \cdot g(x)$ for some $g(x) \in \mathbb{F}_q[x]$ and $t \geq 2$. From Lemma 1, we have that

$$L^{(t)}(x) = \underbrace{L(x) \otimes \cdots \otimes L(x)}_t = (x^{q^n} - 1) \otimes G(x),$$

where $G(x)$ is the linearized q -associate to $g(x)$. In particular $G(x)$ is linearized and then $(x^{q^n} - x) \otimes G(x)$ is divisible by $x^{q^n} - x$ in the ordinary sense. Therefore $L^{(t)}(x) \equiv 0 \pmod{x^{q^n} - x}$ and, since $\deg L(x) < q^n$ and $L(x)$ is nonzero, we conclude that $L(x) \not\equiv 0 \pmod{x^{q^n} - x}$. Thus $L(x)$ is a t -NLP over \mathbb{F}_{q^n} .

Conversely, suppose that $L(x)$ is a t -NLP over \mathbb{F}_{q^n} and set $M(x) = L^{(t)}(x)$. Since $M(x) \in \mathbb{F}_q[x]$ is linearized and vanishes on \mathbb{F}_{q^n} , it follows that $M(x + a) = M(x) + M(a) = M(x)$ for any $a \in \mathbb{F}_{q^n}$. From Proposition 1 there exists a linearized polynomial $R(x) \in \mathbb{F}_q[x]$ such that $M(x) = R(x^{q^n} - x)$, i.e, $M(x) = R(x) \otimes (x^{q^n} - x)$. Therefore

$$L^{(t)}(x) = \underbrace{L(x) \otimes \cdots \otimes L(x)}_t = R(x) \otimes (x^{q^n} - x). \quad (4)$$

Since $R(x) \in \mathbb{F}_q[x]$, from Lemma 1 and equation (4) we conclude that

$$l(x)^t = (x^n - 1)r(x),$$

where $r(x)$ is the conventional q -associate of $R(x)$. Thus $l(x)^t$ is divisible by $x^n - 1$.

Suppose that n is not divisible by p and there exist $t \geq 2$ and $L(x)$ such that $L(x) \in \mathbb{F}_q[x]$ is a t -NLP over \mathbb{F}_{q^n} . In particular, if $L_0(x) = \sum_{i=0}^{n-1} b_i x^i$ is the reduction of $L(x)$ modulo $x^{q^n} - x$, then $L_0(x) \in \mathbb{F}_q[x]$ is also a t -NLP over \mathbb{F}_{q^n} and so $l_0(x) = \sum_{i=0}^{n-1} b_i x^i$, the conventional q -associate of $L_0(x)$, is such that $l_0(x)^t$ is divisible by $x^n - 1$. But if n is not divisible by p , then $x^n - 1$ has only simple roots and so we conclude that $l_0(x)$ is also divisible by $x^n - 1$. Since $l_0(x)$ has degree at most $n - 1$ it follows that $l_0(x) = 0$, hence $L_0(x) = 0$ and so $L(x) \equiv 0 \pmod{x^{q^n} - x}$, a contradiction. \square

Theorem 2 suggests a method for the construction of t -NLP's over \mathbb{F}_{q^n} in the case when n is divisible by p :

Corollary 1. *Let $t \geq 2$ be an integer, $p = \text{char}(\mathbb{F}_{q^n})$ and $n = p^s u$, where $\gcd(u, p) = 1$ and $s \geq 1$. Let $r(x) \in \mathbb{F}_q[x]$ be any nonzero polynomial of degree at most $v = n - 1 - u \cdot \left\lceil \frac{p^s}{t} \right\rceil$ and*

$$l_{r,t}(x) = r(x)(x^u - 1)^{\left\lceil \frac{p^s}{t} \right\rceil}.$$

Then $L_{r,t}(x) \in \mathbb{F}_q[x]$, the linearized q -associate of $l_{r,t}(x)$, is a t -NLP over \mathbb{F}_{q^n} .

Proof. A direct calculation shows that $l_r(x)^t$ is divisible by $x^n - 1$ and $\deg l_r(x) < n - 1$. The result follows from Theorem 2. \square

A simple investigation shows that $v = n - 1 - u \cdot \left\lceil \frac{p^s}{t} \right\rceil \geq 0$ if $n = p^s u$ and $t \geq 2$. The following example is a particular case of Corollary 1 when $r(x) = 1$:

Example 3. *Let $p = \text{char}(\mathbb{F}_{q^n})$, $\alpha \in \mathbb{F}_q^*$ and $n = p^s u$, where $\gcd(u, p) = 1$ and $s \geq 1$. The polynomial*

$$L_{1,t}(x) = \sum_{i=0}^{d_{p,t}} (-1)^{d_{p,t}-i} \binom{d_{p,t}}{i} x^{q^{ui}}$$

is a t -NLP over \mathbb{F}_{q^n} , where $d_{p,t} = \left\lceil \frac{p^s}{t} \right\rceil$.

3. Constructing permutations via t -NLP's

In this section we present a method for constructing permutation polynomials over \mathbb{F}_{q^n} which are the sum of two polynomials, one of them being a t -NLP. A polynomial $f(x) \in \mathbb{F}_{q^n}[x]$ is said to be a permutation polynomial over \mathbb{F}_{q^n} if the map $c \mapsto f(c)$ induced by $f(x)$ is a permutation from \mathbb{F}_{q^n} to itself. We say that a permutation polynomial $f(x)$ is a complete permutation polynomial if $f(x) + x$ is also a permutation polynomial. The set $G(q^n)$ of the permutation polynomials over \mathbb{F}_{q^n} is a group under the polynomial composition modulo $x^{q^n} - x$, and this group is isomorphic to the symmetric group S_{q^n} . The identity element of $(G(q^n), \circ)$ is the identity map $g(x) = x$ and, for each $f \in G(q^n)$, $O(f)$ denotes the order of f in the group $(G(q^n), \circ)$, i.e., $O(f) = \min\{d > 0 \mid f^{(d)}(z) = z, \forall z \in \mathbb{F}_{q^n}\}$.

The following theorem gives an interesting relation between the t -NLP's and some permutation and complete permutation polynomials:

Theorem 3. Let $p = \text{char}(\mathbb{F}_{q^n})$. Let $L(x)$ be a t -NLP over \mathbb{F}_{q^n} and $k(x)$ be any linearized permutation polynomial over \mathbb{F}_{q^n} such that, under the ordinary polynomial composition, k commutes with L , i.e.,

$$k \circ L(x) = L \circ k(x).$$

If $s = O(k)$, then

a) $L(x) + k(x)$ is also a permutation polynomial over \mathbb{F}_{q^n} and its compositional inverse map is given by

$$(L + k)^{(s-1)}(x) = \sum_{i=0}^{t-1} (-1)^i L^{(i)}(k^{(s-1-i)}(x)),$$

where $k^{(0)}(x) = L^{(0)}(x) = x$ and $(s-1-i)$ is taken modulo s .

b) if $k(x)$ is a complete permutation polynomial over \mathbb{F}_{q^n} , then so is $L(x) + k(x)$.

c) $O(L + k)$ divides $\text{lcm}(s, p^e)$, where $e = \lceil \log_p t \rceil$.

d) if $t = 2$ and $\gcd(s, p) = 1$, then $O(L + k) = ps$.

Proof. In the proof of this result and many others in this section we use the following identity:

$$(L + k)^{(p^l)}(z) = L^{(p^l)}(z) + k^{(p^l)}(z)$$

for any $z \in \mathbb{F}_{q^n}$ and $l \in \mathbb{N}$, which is the Frobenius identity in the case when $L(x)$ and $k(x)$ are commuting linearized polynomials over \mathbb{F}_{q^n} .

a) Notice that:

$$\begin{aligned} (L + k) \circ \left[\sum_{i=0}^{t-1} (-1)^i L^{(i)}(k^{(s-1-i)}(z)) \right] &= \sum_{i=0}^{t-1} (-1)^i L^{(i+1)}(k^{(s-1-i)}(z)) + \sum_{i=0}^{t-1} (-1)^i L^{(i)}(k^{(s-i)}(z)) = \\ &= (-1)^{t-1} L^{(t)}(z) + k^{(s)}(z) = 0 + z = z, \end{aligned}$$

for all $z \in \mathbb{F}_{q^n}$. In particular $L + k$ is a permutation over \mathbb{F}_{q^n} and its inverse map is given by $\sum_{i=0}^{t-1} (-1)^i L^{(i)}(k^{(s-1-i)}(x))$.

b) If $k(x)$ is a complete permutation polynomial, then $K(x) = k(x) + x$ is a permutation polynomial and item (a) shows that $L(x) + k(x)$ is a permutation polynomial. A direct calculation shows that $K \circ L(x) = L \circ K(x)$ and then (a) shows that $K(x) + L(x) = (L(x) + k(x)) + x$ is a permutation polynomial. Thus $L(x) + k(x)$ is a complete permutation polynomial.

c) Let $v = O(L + k)$ and $u = \text{lcm}(s, p^e)$, where $e = \lceil \log_p t \rceil$ satisfies $p^e \geq t$. In particular, $L^{(p^e)}(z) = 0$ for any $z \in \mathbb{F}_{q^n}$. Since $p = \text{char}(\mathbb{F}_{q^n})$ and u is divisible by p^e and s , then the following equality holds for any $z \in \mathbb{F}_{q^n}$:

$$(L + k)^{(u)}(z) = ((L + k)^{(p^e)})^{(u/p^e)}(z) = (L^{(p^e)} + k^{(p^e)})^{(u/p^e)}(z) = k^{(u)}(z) = z.$$

Thus $O(L + k) = v$ divides u .

d) Suppose that $t = 2$ and $\gcd(s, p) = 1$. In particular $e = \lceil \log_p t \rceil = 1$ and item (c) shows that $v = O(L + k)$ divides $u = \text{lcm}(s, p) = ps$. Since $L^{(2)}(z) = 0$, for any $z \in \mathbb{F}_{q^n}$ and $d \in \mathbb{N}$ we have the following equality:

$$(L + k)^{(d)}(z) = dL(k^{(d-1)}(z)) + k^{(d)}(z),$$

which is the version of the Binomial Theorem in the case when $L(x)$ and $k(x)$ are commuting linearized polynomials over \mathbb{F}_{q^n} and $L^{(2)}(z) = 0$ for any $z \in \mathbb{F}_{q^n}$. If $v = O(L + k)$ is not divisible by p , then v divides s . Therefore

$$z = (L + k)^{(s)}(z) = sL(k^{(s-1)}(z)) + k^{(s)}(z) = sL(k^{(s-1)}(z)) + z$$

or, equivalently, $sL(k^{(s-1)}(z)) = 0$ for all $z \in \mathbb{F}_{q^n}$. Since $k^{(s-1)}(z)$ is a permutation polynomial over \mathbb{F}_{q^n} and s is not divisible by p , it follows that $L(z) = 0$ for any $z \in \mathbb{F}_{q^n}$, a contradiction with $L(x) \not\equiv 0 \pmod{x^{q^n} - x}$. Thus p divides v and so there exists some divisor s_0 of s such that $v = ps_0$. Therefore, for any $z \in \mathbb{F}_{q^n}$ we have:

$$z = (L + k)^{(ps_0)}(z) = (L^{(p)} + k^{(p)})^{(s_0)}(z) = k^{(ps_0)}(z).$$

Since the equality above holds for all $z \in \mathbb{F}_{q^n}$, it follows that $s = O(k)$ divides $ps_0 = v$. Thus v is divisible by $u = \text{lcm}(s, p) = ps$ and, since v divides $u = ps$ we conclude that $v = u = ps$. \square

In a particular case when $k(x) = \gamma x$, where $\gamma \in \mathbb{F}_q^*$ we have the following:

Corollary 2. *Let $L(x)$ be a t -NLP over \mathbb{F}_{q^n} , $p = \text{char}(\mathbb{F}_{q^n})$ and γ be any element of order $s = \text{ord}_q \gamma$ in the multiplicative group \mathbb{F}_q^* . Then*

- a) $L(x) + \gamma x$ is a permutation polynomial over \mathbb{F}_{q^n} and its compositional inverse map is given by

$$\sum_{i=0}^{t-1} \gamma^{s-1-i} (-1)^i L^{(i)}(x).$$

- b) if $\gamma \neq -1$, then $L(x) + \gamma x$ is also a complete permutation polynomial.
c) $O(L + \gamma x)$ divides $p^e \cdot s$, where $e = \lceil \log_p t \rceil$. Also, if $t = 2$, then $O(L + \gamma x) = ps$.

Proof. Since $\gamma \in \mathbb{F}_q^*$, it follows that γx is a permutation polynomial over \mathbb{F}_{q^n} , commutes with $L(x)$ and satisfies $O(\gamma x) = \text{ord}_q \gamma = s$. Also if $\gamma \neq -1$, γx is a complete permutation polynomial. Finally, since $\text{ord}_q \gamma = s$ divides $q - 1$, we have that $\gcd(s, p) = 1$ and $\text{lcm}(s, p^d) = p^d \cdot s$ for any $d \in \mathbb{N}$. The results now follow directly from Theorem 3. \square

Example 4. *Let $n = 2m$, α and β be elements of $\mathbb{F}_{q^n}^*$ such that $\alpha^{q^m} + \alpha = 0$ and $\beta^{q^m+1} = 1$ and γ be any element of \mathbb{F}_q^* . From Example 2 and Corollary 2, the polynomials*

$$L_{\alpha, \beta, \gamma}(x) = (\alpha \beta x^{q^m} + \alpha x) + \gamma x$$

are permutation polynomials over \mathbb{F}_{q^n} , $O(L_{\alpha, \beta, \gamma}) = p \cdot \text{ord}_q \gamma$ and the compositional inverse map of $L_{\alpha, \beta, \gamma}(x)$ is given by:

$$\gamma^{-1}x - \gamma^{-2}(\alpha \beta x^{q^m} + \alpha x).$$

From Corollary 1, we can construct a large class of permutations:

Corollary 3. Let $t \geq 2$ be an integer, $p = \text{char}(\mathbb{F}_{q^n})$ and $n = p^s u$, where $\gcd(u, p) = 1$ and $s \geq 1$. Let $r(x) \in \mathbb{F}_q[x]$ be any nonzero polynomial of degree at most $v = n - 1 - u \cdot \left\lceil \frac{p^s}{t} \right\rceil$ and

$$l_r(x) = r(x)(x^u - 1)^{\left\lceil \frac{p^s}{t} \right\rceil}.$$

Also, let $L_r(x) \in \mathbb{F}_q[x]$ be the linearized q -associate of $l_r(x)$ and α, β be elements of \mathbb{F}_q^* . Then the polynomials

$$L_{r,\alpha,\beta}(x) = L_r(x) + \alpha \text{Tr}(x) + \beta x$$

are permutation polynomials over \mathbb{F}_{q^n} , where $\text{Tr}(x) = \sum_{i=0}^{n-1} x^{q^i}$ denotes the absolute trace. Moreover if $\beta \neq -1$, then $L_{r,\alpha,\beta}(x)$ is a complete permutation polynomial over \mathbb{F}_{q^n} .

Proof. Since n is divisible by $p = \text{char}(\mathbb{F}_{q^n})$ and $\alpha \in \mathbb{F}_q^*$, a direct calculation shows that the polynomial $\alpha \text{Tr}(x)$ is a 2-NLP over \mathbb{F}_{q^n} . From Corollary 2, $\alpha \text{Tr}(x) + \beta x$ is a permutation over \mathbb{F}_{q^n} and $\alpha \text{Tr}(x) + \beta x$ is also a complete permutation polynomial in the case when $\beta \neq -1$. From Corollary 1, $L_r(x)$ is a t -NLP over \mathbb{F}_{q^n} . But $L_r(x)$ and $\alpha \text{Tr}(x) + \beta x$ belong to $\mathbb{F}_q[x]$ and so these polynomials commute with each other. Now we apply Theorem 3 to $L(x) = L_r(x)$ and $k(x) = \alpha \text{Tr}(x) + \beta x$. \square

In the notation of Corollary 3, we give explicit examples of permutation polynomials over \mathbb{F}_{2^6} and \mathbb{F}_{3^3} of the type $L_{r,\alpha,\beta}(x)$:

$q = t = 2, n = 6$ $r(x)$	$\alpha = \beta = 1$ $L_{r,1,1}(x)$	$q = n = t = 3$ $r(x)$	$\alpha = 1, \beta = -1$ $L_{r,1,-1}(x)$
1	$x^{32} + x^{16} + x^4 + x^2 + x$	1	$x^9 - x^3 - x$
x	$x^{32} + x^8 + x^4$	-1	$x^9 + x$
$x + 1$	$x^{32} + x^4 + x$	x	$-x^9$
x^2	$x^{16} + x^8 + x^2$	$-x$	$-x^3$
$x^2 + 1$	$x^{16} + x^2 + x$	$x + 1$	$-x^9 + x^3 - x$
$x^2 + x$	x^8	$x - 1$	$-x^9 - x^3 + x$
$x^2 + x + 1$	x	$-x + 1$	$x^3 + x$
		$-x - 1$	$-x$

3.1. Cycle Structure

If F is any function from a finite set S to itself, we can associate to it a directed graph $G(F, S)$ with vertex set S and edge set $\{(x, F(x))\}_{x \in S}$. We say that $G(F, S)$ is the *functional graph* associated to F . If $f(x)$ is a permutation polynomial over \mathbb{F}_{q^n} , it can be verified that the graph $G_f := G(f, \mathbb{F}_{q^n})$ is decomposed into disjoint cycles. Moreover, $O(f)$ is the least common multiple of the cycle lengths of G_f and the vertex of G_f associated to $a \in \mathbb{F}_{q^n}$ belongs to a cycle of length d if, and only if, d is the least positive integer such that $f^{(d)}(a) = a$.

If $L(x)$ and $k(x)$ are linearized polynomials over \mathbb{F}_{q^n} as in Theorem 3, we know that $L(x) + k(x)$ is a permutation polynomial over \mathbb{F}_{q^n} . What is the relation between the functional graphs G_k and G_{L+k} ?

In the case when $L(x)$ is a 2-NLP over \mathbb{F}_{q^n} , the following theorem shows that the cycle lengths of G_{L+k} cannot be much larger than the ones of G_k and, imposing an additional condition on $O(k)$, we can completely describe the cycle structure of G_{L+k} from G_k .

Theorem 4. *Let be a 2-NLP over \mathbb{F}_{q^n} and let $k(x)$ be any linearized permutation polynomial over \mathbb{F}_{q^n} such that, under the ordinary polynomial composition, $k(x)$ commutes with $L(x)$, i.e., $k \circ L(x) = L \circ k(x)$. Set $s = O(k)$ and $p = \text{char}(\mathbb{F}_{q^n})$. Suppose that the vertex associated to an element $a \in \mathbb{F}_{q^n}$ belongs to cycles of lengths m_a and m'_a in G_k and G_{L+k} , respectively. Then the following holds:*

- a) m'_a divides $\text{lcm}(m_a, p)$ and, if $L(a) = 0$, then $m_a = m'_a$.
- b) if $\text{gcd}(s, p) = 1$ then $m'_a = \begin{cases} m_a & \text{if } L(a) = 0 \\ pm_a & \text{otherwise.} \end{cases}$

Proof. a) Let $v = \text{lcm}(m_a, p)$. Notice that $(L + k)^{(v)}(z) = (L^{(p)} + k^{(p)})^{(v/p)}(z) = k^{(v)}(z)$ for any $z \in \mathbb{F}_{q^n}$. Since m_a divides v , it follows that $k^{(v)}(a) = a$, hence $(L + k)^{(v)}(a) = a$ and so m'_a divides v . If $L^{(2)}(z) = 0$, we have seen that

$$(L + k)^{(d)}(z) = dk^{(d-1)}(L(z)) + k^{(d)}(z),$$

for any $d \in \mathbb{N}$ and $z \in \mathbb{F}_{q^n}$. Therefore, if $L(a) = 0$ then $(L + k)^{(d)}(a) = k^{(d)}(a)$. Thus $m'_a = m_a$ if $L(a) = 0$.

b) If $L(a) \neq 0$, item (a) shows that $m_a = m'_a$. Suppose that $L(a) \neq 0$ and that m'_a is not divisible by p . It follows from item (a) that m'_a divides m_a and then

$$a = (L + k)^{(m_a)}(a) = m_a L(k^{(m_a-1)}(a)) + k^{m_a}(a) = m_a k^{(m_a-1)}(L(a)) + a,$$

hence $m_a k^{(m_a-1)}(L(a)) = 0$. Now, since $\text{gcd}(s, p) = 1$ and m_a divides s , it follows that m_a is not divisible by p , hence $k^{(m_a-1)}(L(a)) = 0$. Notice that $k^{(m_a-1)}(x)$ is a linearized permutation polynomial and then maps the zero element to itself. Since $L(a) \neq 0$, it follows that the composition $k^{(m_a-1)}(L(a))$ is never zero and so we get a contradiction. Thus p divides m'_a and then there exists an integer u such that $m'_a = pu$. Therefore

$$a = (L + k)^{(pu)}(a) = (L^{(p)} + k^{(p)})^{(u)}(a) = k^{(pu)}(a),$$

and then m_a divides pu . Since m_a is not divisible by p it follows that m_a divides u , hence pm_a divides $pu = m'_a$. Item (a) shows that m'_a divides $\text{lcm}(m_a, p) = pm_a$ and thus $m'_a = pm_a$. \square

In the case when $k(x) = \gamma x$ for some $\gamma \in \mathbb{F}_q^*$, we can determine precisely the graphs G_{L+k} :

Corollary 4. *Let $L(x)$ be a 2-NLP over \mathbb{F}_{q^n} and γ be an element of order s in the multiplicative group \mathbb{F}_q^* . Then the functional graph $G_{L+\gamma x}$ has one cycle of length 1, $\frac{z_L - 1}{s}$ cycles of length s and $\frac{q^n - z_L}{ps}$ cycles of length ps , where $z_L = \#Z_L$ is the number of roots of L in \mathbb{F}_{q^n} . In particular, if L_1 and L_2 are 2-NLP's over \mathbb{F}_{q^n} and $\gamma_1, \gamma_2 \in \mathbb{F}_q^*$, then the graphs $G_{L_1+\gamma_1 x}$ and $G_{L_2+\gamma_2 x}$ have the same cycle structure (hence isomorphic) if, and only if, $z_{L_1} = z_{L_2}$ and $\text{ord}\gamma_1 = \text{ord}\gamma_2$.*

Proof. For the first statement, notice that any nonzero element belongs to a cycle of length s in $G_{\gamma x}$ and the zero element is a fixed point. Since $O(\gamma x) = s$ and s divides $q - 1$, we have that $\gcd(d, p) = 1$ and now the result follows from part b) of Theorem 4. The second statement follows directly from the first. \square

3.2. Involutions in binary fields

Here we are interested in the construction of involutions over binary fields with no fixed points. Let q be a power of 2 and $L(x)$ be any 2-NLP over \mathbb{F}_{q^n} . From Theorem 3 we know that $L(x) + x$ is a permutation polynomial over \mathbb{F}_{q^n} and it can be verified that $L(x) + x$ is in fact an involution over \mathbb{F}_{q^n} . However, $L(x) + x$ has many fixed points which are exactly the roots of $L(x)$ over \mathbb{F}_{q^n} . The following proposition shows how to completely eliminate those fixed points:

Proposition 2. *Let \mathbb{F}_{q^n} be a finite field such that $\text{char}(\mathbb{F}_{q^n}) = 2$ and $L(x)$ be any 2-NLP over \mathbb{F}_{q^n} such that $V_L \subsetneq Z_L$. Then, for any $a \in Z_L \setminus V_L$, the polynomial $f(x) = L(x) + x + a$ is an involution over \mathbb{F}_{q^n} with no fixed points. In particular, if $\dim_{\mathbb{F}_q} V_L < n/2$ then there is some element $b \in Z_L \setminus V_L$.*

Proof. Since $L(a) = 0$ and $\text{char}(\mathbb{F}_{q^n}) = 2$, a direct calculation shows that $f(x) = L(x) + x + a$ is an involution over \mathbb{F}_{q^n} . If $f(x)$ has a fixed point $\alpha \in \mathbb{F}_{q^n}$, then $f(\alpha) = \alpha$ and so $L(\alpha) = a$, which is impossible since $a \notin V_L$. Thus $f(x)$ has no fixed points.

Since $L^{(2)}(z) = 0$ for any $z \in \mathbb{F}_{q^n}$ we have that $V_L \subset Z_L$. If $\dim_{\mathbb{F}_q} V_L < n/2$ then $\dim_{\mathbb{F}_q} Z_L = n - \dim_{\mathbb{F}_q} V_L > n/2$ and so $V_L \subsetneq Z_L$. Thus there is some element $b \in Z_L \setminus V_L$. \square

In particular we have the following:

Corollary 5. *Let q be a power of 2 and let $k = \mathbb{F}_{q^m}$ and $K = \mathbb{F}_{q^n}$ be fields such that $k \subset K$ and $m < n/2$. If θ is an element of $\mathbb{F}_{q^n}^*$ and $\text{Tr}_{K/k}(\theta) = 0$, then there exists an element $\alpha \in \mathbb{F}_{q^n}$ such that $\text{Tr}_{K/k}(\alpha) = 0$ and $\alpha \notin \theta \cdot \mathbb{F}_{q^m}$. In particular,*

$$f(x) = \theta \cdot \text{Tr}_{K/k}(x) + x + \alpha$$

is a involution over \mathbb{F}_{q^n} with no fixed points.

Proof. In the notation of Proposition 2, take $L(x) = \theta \cdot \text{Tr}_{K/k}(x)$ and notice that $V_L = \theta \cdot \mathbb{F}_{q^m}$ has dimension $m < n/2$ as an \mathbb{F}_q -vector space. Now the result follows directly from Proposition 2. \square

The corollary above suggests explicit constructions of involutions with no fixed points which can be represented by *sparse polynomials*, i.e., polynomials with few nonzero coefficients. For instance, let m be any positive integer and $n = 4m$. If $f(x)$ is any irreducible polynomial over \mathbb{F}_2 and has degree n , then $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(f(x)) = \mathbb{F}_2[\beta]$, where β is the coset of x in the quotient $\mathbb{F}_2[x]/(f(x))$. Take $K = \mathbb{F}_{2^n}$ and $k = \mathbb{F}_{2^m}$, hence

$$\text{Tr}_{K/k}(x) = x^{2^{3m}} + x^{2^{2m}} + x^{2^m} + x.$$

A direct calculation shows that $\text{Tr}_{K/k}(1) = \text{Tr}_{K/k}(\beta^{2^m} + \beta) = 0$. But if $\beta^{2^m} + \beta \in \mathbb{F}_{2^m}$ then

$$\beta^{2^{2m}} + \beta^{2^m} = (\beta^{2^m} + \beta)^{2^m} = \beta^{2^m} + \beta,$$

hence $\beta^{2^{2m}} = \beta$, i.e., $\beta \in \mathbb{F}_{2^{2m}}$. Therefore $\mathbb{F}_{2^n} = \mathbb{F}_2[\beta] \subset \mathbb{F}_{2^{2m}}$, a contradiction since $n = 4m$. In conclusion, $\beta^{2^m} + \beta \notin \mathbb{F}_{2^{2m}}$ and then taking $\alpha = \beta^{2^m} + \beta$ and $\theta = 1$ as in Corollary 5 we have that

$$f(x) = x^{2^{3m}} + x^{2^{2m}} + x^{2^m} + \beta^{2^m} + \beta$$

is an involution over $\mathbb{F}_{2^n} = \mathbb{F}_2[\beta]$ with no fixed points.

Example 5. Let $\mathbb{F}_{2^{32}} = \mathbb{F}_2[x]/(x^{32} + x^7 + x^3 + x + 1) = \mathbb{F}_2[\beta]$, where β is the coset of x in the quotient $\mathbb{F}_2[x]/(x^{32} + x^7 + x^3 + x + 1)$. The polynomial

$$f(x) = x^{2^{24}} + x^{2^{16}} + x^{2^8} + \beta^{2^8} + \beta$$

is an involution over $\mathbb{F}_{2^{32}}$ and has no fixed points.

References

- [1] C. Boura, A. Canteaut, L.R. Knudsen, *Reflection Ciphers* Des. Codes Cryptogr. (2015), doi:10.1007/s10623-015-0143-x.
- [2] Y. Laigle-Chapuy, *Permutation polynomials and applications to coding theory*, Finite Fields Appl. 13 (2007) 58-70.
- [3] R. Lidl, H. Niederreiter, *Introduction to finite fields and their applications*. Cambridge University Press New York, NY, USA 1986.
- [4] Gary L. Mullen, Daniel Panario *Handbook of Finite Fields*. Taylor and Francis, Boca Raton, 2013.
- [5] J. Schwenk, K. Huber, *Public key encryption and digital signatures based on permutation polynomials*, Electron. Lett. 34 (1998) 759-760.